UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,874	12/14/2001	Jonathan Edwards	19903.0011	1766

23517 7590 10/05/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/014,874	EDWARDS ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) *3-5, 15-17 and 27-29* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 6-14, 18-26 and 30-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on June 29, 2005. Claims 3 – 5, 15 – 17 and 27 – 29 have been cancelled. Claims 1, 6 – 13, 18 – 25 and 30 – 36 have been amended and new Claims 37 – 39 are added. Therefore, Claims 1, 2, 6 – 14, 18 – 26 and 29 – 39 are pending.

Drawings

2. The amended drawings were received on June 29, 2005. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: Item #420 and #422, Fig. 4, Replacement sheet. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The substitute specification filed June 29, 2005 has not been entered because it does not conform to 37 CFR 1.125(b) and (c) because:

Substitution specification does not provide details on steps 420 – 422. Applicant has to explicitly disclose the conditions for repetition of steps 420 – 422.

Substitution specification discloses, "If, in step 406, ... Thus, steps 412 – 416 may be repeated. As is inherent and/or obvious to one of ordinary skill, such repetition may repeat until the process is complete. Note steps 420 – 422.", it is not clear whether steps 410 – 420 may be repeated until the process is complete, as shown in Fig. 4, Replacement sheet or 412 – 416 may be repeated as shown in Fig. 4 as originally filed.

Examiner requests clarification and denies entry of the amended specification.

Claim Objections

4. Claims 6 – 9, 12, 18 – 20, 27 – 29 and 36 – 39 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim limitations "at least one file that is not needed to perform the decryption, decompression, or unpacking comprises the system library file.", "at least one file that is

not needed to perform the decryption, decompression, or unpacking comprises the executable file not related to the process.", "at least one file that is not needed to perform the decryption, decompression, or unpacking comprises the data file not related to the process." and "scanning the process for a malware before execution of the process", have been recited in the independent Claims 1, 13 and 25.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 2, 6 – 14, 18 – 26 and 29 – 39 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 1, 13 and 25 read, " ...an anti-malware program ..." and "... encryption, compression, or packing is carried out by an entity separate from the anti-malware program; ...".

With respect to "an anti-malware program", although the specification discloses the term "an anti-virus program" that includes virus scanning routines and virus removal

routines (instant application, Page 6 lines 12 – 19), the specification does not disclose an anti-malware program. Applicant's amendment does not clarify how an anti-malware program can interrupt the process for a malware.

With respect to "encryption, compression, or packing is carried out by an entity separate from the anti-malware program", although the specification discloses "... other process files, such as process files 208C-Z may include encrypted code or compressed or packed code and/or data." (instant application, Page 7 lines 10 – 20), the specification does not disclose encryption, compression, or packing is carried out by an entity separate from the anti-malware program. Applicant's amendment does not clarify how encryption, compression, or packing is carried out by an entity separate from anti-malware program.

For Examination purposes, anti-malware program is broadly interpreted as an anti-virus program to scan the process.

The dependent claims 2, 6 – 12, 14, 18 – 24, 26 and 30 – 39 are rejected at least by virtue of their dependency on the dependent claims.

Response to Remarks/Arguments

6. Applicant's arguments filed 6/29/2005 have been fully considered but they are not persuasive for the following reasons:

7. Regarding currently amended claims 1, 13 and 25, Applicant argues that the Drake do not teach "anti-malware program for interrupting the execution of process", "interrupting execution of the process when the process accesses at last one file that is not needed to perform decryption, decomposition and unpacking, wherein encryption, compression, or packing is carried out by an entity separate from the anti-malware program" and "wherein the at least one file is selected form the group consisting of a system library file, and executable file not related to the process, and a data file not related to the process". These arguments are not found persuasive.

Drake discloses "detecting tampering and preventing execution-tracing" through the use of scanning at the beginning of execution or continuously (repeating scanning process) upon certain events to replace insecure routines (processes) (Drake Column 4 lines 48 – 65). Drake also discloses scanning the command environment and the execution instruction by detecting debuggers and other operating system processes (other file not related to the process). Drake further discloses that combining detecting tampering and preventing execution-tracing with encryption to successfully decrypt the executable process (Drake Column 7 line 53 – Column 8 line 48).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "anti-malware program for interrupting the execution of process", "interrupting execution of the process when the process accesses at last one file that is not needed to perform decryption, decomposition and unpacking, wherein encryption, compression, or packing is carried out by an entity separate from the anti-malware program" and "wherein the at least one file is selected

form the group consisting of a system library file, and executable file not related to the process, and a data file not related to the process", broadly recited in the amended independent claims 1, 13 and 25. The dependent claims 2, 6 – 12, 14, 18 – 24, 26 and 30 – 39 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 1, 2, 6 – 14, 18 – 26 and 30 – 39 is respectfully maintained.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1, 2, 6 – 14, 18 – 26 and 30 – 39 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Drake (U.S. Patent Number 6,006,328).

9. As per Claim 1, Drake teaches

interrupting execution of a process that has been loaded for execution, wherein the execution of the process is interrupted by an anti-malware program (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43);

wherein execution of the process comprises the step of: loading code for execution by the process from a compressed, packed or encrypted file (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the step of interrupting execution of the process comprises the step of: interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking after decryption, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the at least one file is selected form the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

10. As per Claim 13, Drake teaches

a processor operable to execute computer program instructions (Column 9 lines 50 – 57);

a memory operable to store computer program instructions executable by the processor (Column 9 lines 50 – 57); and

computer program instructions stored in the memory and executable to perform the steps of:

interrupting execution of a process that has been loaded for execution wherein the execution of the process is interrupted by an anti-malware program (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43); wherein execution of the process comprises the step of: loading code for execution by the process from a compressed, packed or encrypted file (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the step of interrupting execution of the process comprises the step of: interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking after decryption, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the at least one file is selected form the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

11. As per Claim 25, Drake teaches

a computer readable medium (Column 8 lines 24 – 30);

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

interrupting execution of a process that has been loaded for execution wherein the execution of the process is interrupted by an anti-malware program (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43); wherein execution of the process comprises the step of: loading code for execution by the process from a compressed, packed or encrypted file (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the step of interrupting execution of the process comprises the step of: interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking after decryption, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program (Column 4 lines 47 – 65 and Column 6 lines 6 – 32);

wherein the at least one file is selected form the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

12. As per Claims 2, 14 and 26, Drake further teaches wherein the process is associated with an application program (Column 9 lines 50 – 57).

13. As per Claims 6, 18 and 30, Drake further teaches wherein the at least one tile that is not needed to perform the decryption, decompression, or unpacking comprises the system library file (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

14. As per Claims 7, 19 and 31, Drake further teaches wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises the executable file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

15. As per Claims 8, 20 and 32, Drake further teaches wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises the data file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

16. As per Claims 9, 21 and 33, Drake further teaches wherein the malware is a computer virus (Column 1 line 56 – Column 2 line 62).

17. As per Claims 10, 22 and 34, Drake further teaches wherein the malware is a computer worm (Column 1 line 56 – Column 2 line 62).

18. As per Claims 11, 23 and 35, Drake further teaches wherein the malware is a Trojan horse program (Column 1 line 56 – Column 2 line 62).

19. As per Claims 12, 24 and 36, Drake further teaches scanning the process for a malware before execution of the process (Column 1 line 56 – Column 2 line 62 and Column 3 lines 33 – 67).

20. As per Claim 39, Drake further teaches wherein the interrupting of the execution of the process is performed before any malware in the loaded code has a chance to perform any malicious or unauthorized actions (Column 4 lines 47 – 65).

21. As per Claim 37, Drake further teaches terminating the process if malware is found before execution of the process (Column 1 line 56 – Column 2 line 62 and Column 3 lines 33 – 67).

22. As per Claim 38, Drake teaches performing anti-virus processing on the process if malware is found; wherein the anti-virus processing includes at least one of quarantining, cleaning, and deleting files storing the loaded code (Column 4 line 47 – Column 5 line 15).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

23. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

24. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
September 21, 2005.

Primary Examiner
AU 2131
10/21/05